PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2003-036243**
(43)Date of publication of application : **07.02.2003**

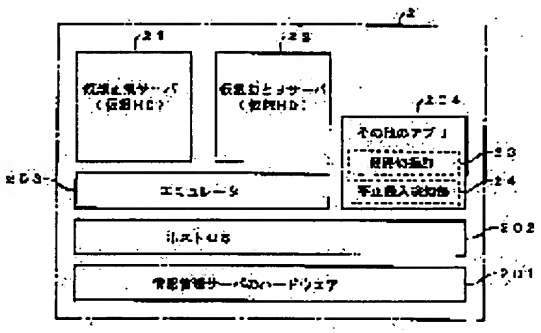
(51)Int.Cl. **G06F 15/00**
H04L 12/66

(21)Application number : **2001-222690**
(22)Date of filing : **24.07.2001**

(71)Applicant : **KDDI CORP**
(72)Inventor : **TAKEMORI KEISUKE**
TANAKA TOSHIAKI
KIYOMOTO SHINSAKU
NAKAO KOJI

(54) **FIRE WALL SYSTEM**

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a fire wall system to prevent unauthorized access to a normal server without making the lurker to be aware of the failure of the unauthorized access.
SOLUTION: A host OS 202 operates on hardware 201 of an information management server 2. On the host OS 202, an emulator 203 operates together with various kinds of applications 204. On the emulator 203, a virtual normal server 21 and a virtual decoy server 22 operate as independent hardware servers and unique IP addresses are assigned to each of them. A normal access to the information management server 2 is led to the virtual normal server 21, while an unauthorized access is led to the virtual decoy server 22.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－36243
（P2003－36243A）
(43)公開日　平成15年２月７日(2003.2.7)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ａ	５Ｂ０８５
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　12/66	Ｂ	５Ｋ０３０

審査請求　未請求　請求項の数５　ＯＬ　（全９頁）

(21)出願番号　特願2001－222690(P2001－222690)

(22)出願日　平成13年７月24日(2001.7.24)

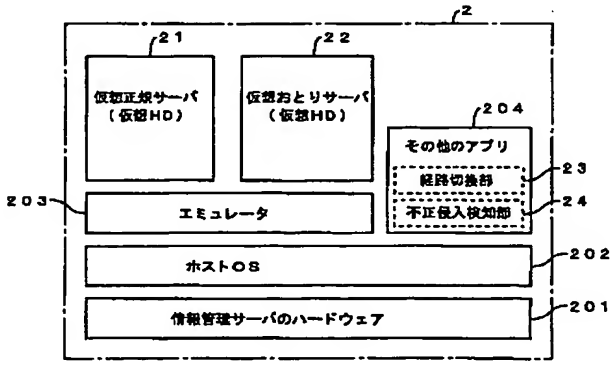
特許法第30条第１項適用申請有り　2001年２月20日　社団法人情報処理学会発行の「情報処理学会研究報告　情処研報　Ｖｏｌ．2001，　Ｎｏ．16」に発表

(71)出願人　000208891
ケイディーディーアイ株式会社
東京都新宿区西新宿二丁目３番２号
(72)発明者　竹森　敬祐
埼玉県上福岡市大原二丁目１番15号　株式会社ケイディーディーアイ研究所内
(72)発明者　田中　俊昭
埼玉県上福岡市大原二丁目１番15号　株式会社ケイディーディーアイ研究所内
(74)代理人　100084870
弁理士　田中　香樹　（外１名）

最終頁に続く

(54)【発明の名称】　不正侵入防止システム

(57)【要約】
【課題】　正規サーバへの不正侵入を防止し、かつ不正侵入者に不正侵入の失敗を悟られないようにした不正侵入防止システムを提供する。
【解決手段】　情報管理サーバ２のハードウエア２０１上ではホストＯＳ２０２が動作する。ホストＯＳ２０２上では各種のアプリケーション２０４と共にエミュレータ２０３が動作する。エミュレータ２０３上では、仮想正規サーバ２１および仮想おとりサーバ２２が、独立したハードウエアによるサーバとして動作し、それぞれに固有のＩＰアドレスが付与される。情報管理サーバ２への正規アクセスは仮想正規サーバ２１へ誘導され、不正アクセスは仮想おとりサーバ２２へ誘導される。



1

【特許請求の範囲】
【請求項１】　ネットワークに接続されたホストサーバへの不正侵入を防止する不正侵入防止システムにおいて、
前記ホストサーバ上に仮想的に設けられた仮想正規サーバおよび仮想おとりサーバと、
前記ホストサーバへの正規アクセスを前記仮想正規サーバへ誘導し、不正アクセスを前記仮想おとりサーバへ誘導する経路切換手段とを具備し、
前記仮想正規サーバおよび仮想おとりサーバが実質的に同一のディレクトリ構造を有することを特徴とする不正侵入防止システム。
【請求項２】　前記経路切換手段は、ホストサーバ宛のアクセスを前記正規サーバまたはおとりサーバへ誘導し、前記各サーバからの応答の発信元アドレスを前記ホストサーバのアドレスに書き換えることを特徴とする請求項１に記載の不正侵入防止システム。
【請求項３】　前記仮想正規サーバおよび仮想おとりサーバには、相互に異なるアドレスが付与されたことを特徴とする請求項１または２に記載の不正侵入防止システム。
【請求項４】　ネットワークに接続されたホストサーバへの不正侵入を防止する不正侵入防止システムにおいて、
異なるアドレスで管理される正規サーバおよびおとりサーバと、
前記正規サーバ宛のパケットを、不正アクセスが検知されるまでは、前記正規サーバおよびおとりサーバの双方へ転送し、不正アクセスが検知されると、おとりサーバのみへ転送する経路切換手段とを具備し、
前記経路切換手段はさらに、前記不正アクセスが検知されるまでは、前記各サーバからの応答が揃った以降に正規サーバからの応答を返送し、前記不正アクセスが検知されると、前記おとりサーバからの応答を返送することを特徴とする不正侵入防止システム。
【請求項５】　ネットワークに接続されたホストサーバへの不正侵入を防止する不正侵入防止システムにおいて、
前記ホストサーバ上の異なる領域に設けられた正規データ領域およびおとりデータ領域と、
前記正規データ領域に対する不正アクセスを検知して、前記おとりデータ領域を対象にchrootをコールする手段と、
前記不正アクセスを前記おとりデータ領域へ誘導する手段とを具備し、
前記おとりデータ領域が、前記正規データ領域のルートディレクトリ以下のディレクトリ構造に対応したディレクトリ構造を所定の基準ディレクトリ以下に有し、
前記chrootの実行により、前記おとりサーバ領域の基準ディレクトリが仮想的なルートディレクトリに変換されることを特徴とする不正侵入防止システム。

2

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワーク上のホストサーバに悪意の第三者が不正侵入し、さらにはその内容を改竄、破壊等することを防止する不正侵入防止システムに係り、特に、不正侵入者に不正侵入の失敗を悟られること無く、これを確実に防止できる不正侵入防止システムに関する。
【０００２】
【従来の技術】近年、ホームページの改竄に代表される情報管理サーバへの不正侵入が後を立たない。このような問題点を解決するために、従来は、不正侵入者の通信セッションを情報管理サーバ内に侵入させない対策が講じられていた。例えば、情報管理サーバの不必要なポートを閉めることで攻撃されやすい経路を塞いだり、ファイアーウォールを設けて不正侵入者の通信セッションをフィルタリングしたり、あるいは不正侵入者の通信セッションを切断することなどが行われてきた。
【０００３】しかしながら、上記した従来の侵入防止システムでは、不正侵入者は侵入に失敗したことを認知できるため、他の侵入方法で再度侵入を試みたり、あるいは侵入を諦める代わりに大量の通信セッションを集中させ、サーバをダウンさせるなどの破壊工作や妨害工作に転じる場合があった。
【０００４】このような技術課題を解決するために、本来の情報管理サーバの近傍に、故意に侵入し易くしたおとりサーバを配置し、当該おとりサーバでの改竄を許容することで、情報管理サーバへの不正侵入を防止すると共に、不正侵入者に不正侵入の失敗を悟られないようにした技術が提案されている（Network Associates社製のCyberCop Sting：米国）。
【０００５】しかしながら、本来の情報管理サーバの近傍におとりサーバを配置する構成では、おとりサーバへの侵入を情報管理サーバへの侵入よりも簡単にすることで、不正侵入者をおとりサーバへおびき寄せているに過ぎない。このため、不正侵入者におとりサーバを見破られ、改めて情報管理サーバを攻撃されると、従来と同様に情報管理サーバへ侵入されてしまうという問題があった。
【０００６】さらに、おとりサーバは、その挙動が本来のサーバとは微妙に異なるために、その応答に含まれるディレクトリ情報等に基づいて、おとりサーバへの誘導を見破られてしまう可能性があった。このため、改めて正規サーバを攻撃されると、従来と同様に正規サーバへ侵入されてしまうという問題があった。
【０００７】このような技術課題を解決するために、本発明の発明者等は、情報管理サーバの内部に正規領域とおとり領域とを用意して、コマンドのアクセス情報を制御することで、不正侵入者のセッションをおとり領域へ

と誘導するシステム（従来技術Ａ）を発明し、これを特許出願（特願２０００－２９９５５５号）した。

【０００８】さらに、ネットワーク上に正規サーバとおとりサーバとを用意し、スイッチシステムによって不正侵入者のセッションをおとりサーバへ誘導するシステム（従来技術Ｂ）を発明し、これを特許出願（特願２０００－２９９５５６号）した。

【０００９】

【発明が解決しようとする課題】従来技術Aのように、情報管理サーバ内部に２つの領域を設け、コマンドのアクセス先を制御しておとり領域へと誘導する機能を実現する場合、全てのコマンド／レスポンスの組み合せを考慮した作り込みが必要であり、システムが複雑になるという技術課題があった。

【００１０】従来技術Ｂのように、ネットワーク上に正規サーバとおとりサーバとを併設するシステムでは、不正侵入者および正規サーバ間の通信と不正侵入者およびおとりサーバ間の通信とに関する整合性を確保しなければならないので、システム構成が複雑になるという技術課題があった。

【００１１】さらに、各従来技術に共通して、危険な通信セッションと言い切れない疑わしい通信セッションの取り扱いの判断が難しく、対策が遅れてしまうという技術課題があった。

【００１２】本発明の目的は、上記した従来技術の課題を解決し、正規サーバへの不正侵入を防止し、かつ不正侵入者に不正侵入の失敗を悟られないようにした不正侵入防止システムを提供することにある。

【００１３】

【課題を解決するための手段】上記した目的を達成するために、本発明は、ネットワークに接続されたホストサーバへの不正侵入を防止する不正侵入防止システムにおいて、以下のような手段を講じた点に特徴がある。

【００１４】(1)ホストサーバ上に仮想的に設けられた仮想正規サーバおよび仮想おとりサーバと、前記ホストサーバへの正規アクセスを前記仮想正規サーバへ誘導し、不正アクセスを前記仮想おとりサーバへ誘導する経路切換手段とを具備し、前記仮想正規サーバおよび仮想おとりサーバが実質的に同一のディレクトリ構造を有することを特徴とする。

【００１５】(2)異なるアドレスで管理される正規サーバおよびおとりサーバと、前記正規サーバ宛のパケットを、不正アクセスが検知されるまでは、前記正規サーバおよびおとりサーバの双方へ転送し、不正アクセスが検知されると、おとりサーバのみへ転送する経路切換手段とを具備し、前記経路切換手段はさらに、前記不正アクセスが検知されるまでは、前記各サーバからの応答が揃った以降に正規サーバからの応答を返送し、前記不正アクセスが検知されると、前記おとりサーバからの応答を返送することを特徴とする。

【００１６】(3)ホストサーバ上の異なる領域に設けられた正規データ領域およびおとりデータ領域と、正規データ領域に対する不正アクセスを検知して、前記おとりデータ領域を対象にchrootをコールする手段と、前記不正アクセスを前記おとりデータ領域へ誘導する手段とを具備し、前記おとりデータ領域が、前記正規データ領域のルートディレクトリ以下のディレクトリ構造に対応したディレクトリ構造を所定の基準ディレクトリ以下に有し、前記chrootの実行により、前記おとりサーバ領域の基準ディレクトリが仮想的なルートディレクトリに変換されることを特徴とする。

【００１７】上記した特徴(1)によれば、正規サーバとおとりサーバとが物理的には同一のサーバ上に構築されているのにもかかわらず独立したサーバとして機能するので、両者のディレクトリ構造を同一にできる。したがって、おとりサーバは正規サーバをコピーするだけで簡単に構築できる。

【００１８】また、両者はディレクトリ構造が同一なので、アクセス先が正規サーバおよびおとりサーバのいずれかにかわらず、応答に含まれるディレクトリ情報が同一となる。したがって、不正侵入者に不正侵入の失敗を悟られず、同一の不正侵入者による更なる不正侵入行為、破壊行為あるいは迷惑行為等から守ことができる。

【００１９】上記した特徴(2)によれば、正規サーバとおとりサーバとの整合性が常に保たれるので、不正侵入者によるアクセスをおとりサーバへ誘導しても、これを各サーバの不整合に基づいて悟られることがない。

【００２０】上記した特徴(3)によれば、正規データ領域とおとりデータ領域とが同一のサーバ上に構築されているにもかかわらず、侵入者から観察されるディレクトリ構造を実質的に同一にできる。したがって、不正侵入者によるアクセスをおとりサーバへ誘導し、当該おとりデータ領域から応答しても、この応答に含まれるアクセス先のディレクトリ情報に基づいて不正侵入の失敗を悟られることがない。

【００２１】

【発明の実施の形態】以下、図面を参照して本発明の好ましい実施の形態について説明する。図１は、本発明を適用した不正侵入防止システムの第１実施形態のブロック図である。

【００２２】通信ネットワーク１には、本発明の不正侵入防止システムが適用される情報管理サーバ（ホストサーバ）２と、当該情報管理サーバ２に対して通信ネットワーク１を介して接続された複数の通信端末３（３ａ、３ｂ…）とが接続されている。前記情報管理サーバ２は、悪意の第三者による不正侵入から保護すべき仮想正規サーバ２１と、前記仮想正規サーバ域２１に対する不正アクセスを身代わりとなって受け入れる仮想おとりサーバ２２と、パスワードの間違え回数が基準値を越えたアクセスや、ポートスキャンを実行したアクセス等を不

正侵入者によるアクセスと判定し、その旨を経路切換部２３へ通知する不正侵入検知部２４と、前記情報管理サーバ２への正規アクセスを前記仮想正規サーバ２１へ誘導し、不正アクセスを前記仮想おとりサーバ２２へ誘導する経路切換部２３とを含む。

【００２３】図２は、前記情報管理サーバ２の構造を模式的に示したブロック図であり、前記と同一の符号は同一または同等部分を表している。

【００２４】情報管理サーバ２のハードウエア２０１上ではホストＯＳ２０２が動作する。このホストＯＳ２０２上では、前記経路切換部２３および不正侵入検知部２４を含む各種のアプリケーション２０４と共に、当該情報管理サーバ２上に仮想的なハードウエア環境を構築するエミュレータ２０３が動作する。そして、本実施形態では、前記仮想正規サーバ２１および仮想おとりサーバ２２が、前記エミュレータ２０３上で独立したハードウエア（ハードディスク：ＨＤ）によるサーバとして動作する。

【００２５】本実施形態では、前記エミュレータ２０３として、米国のＶＭｗａｒｅ² 社により開発されたエミュレータ「ＶＭｗａｒｅ」（http://www.vmware.com）を採用している。

【００２６】上記した構成によれば、前記仮想正規サーバ２１および仮想おとりサーバ２２は、同一のハードウエア上に構築されるにもかかわらず、相互に異なるＩＰアドレスを付与することが可能になる。また、仮想おとりサーバ２２は、前記仮想正規サーバ２１の内容をコピーすることにより簡単に構築することができ、そのディレクトリ構造を、図３に示したように、仮想正規サーバ２１と実質的に同一にできる。

【００２７】次いで、本実施形態の動作を、図４，５に示した通信シーケンスを参照して説明する。なお、ここでは正規利用者のＩＰアドレスが「０１」、以下同様に、情報管理サーバ２が「０２」、仮想正規サーバが「０３」、仮想おとりサーバが「０４」、不正利用者が「０５」であるものとして説明する。

【００２８】正規利用者によるアクセスの場合、図４に示したように、正規利用者端末３ａからは、発信元アドレスが正規利用者のＩＰドレス「０１」、宛先アドレスが情報管理サーバ２のＩＰアドレス「０２」であるパケット構造のコマンドが送出される。情報管理サーバ２の経路切換部２３は、受信パケットにかかる通信セションが不正侵入と認識されていなければ、その宛先アドレス「０２」を仮想正規サーバ２１のＩＰアドレス「０３」に書き換えて転送する。

【００２９】仮想正規サーバ２１は、当該パケットを受信して所定の処理を実行すると、発信元アドレスが自身のＩＰドレス「０３」、宛先アドレスが正規利用者端末３ａのＩＰドレス「０１」であるパケット構造の応答を返送する。経路切換部２３は、受信パケットの発信元アドレス「０３」を情報管理サーバ２のＩＰアドレス「０２」に書き換えて返送する。

【００３０】これに対して、不正利用者によるアクセスの場合、図５に示したように、不正利用者端末３ｂからは、発信元アドレスが不正利用者のＩＰドレス「０５」、宛先アドレスが情報管理サーバ２のＩＰドレス「０２」であるパケットが送出される。情報管理サーバ２の経路切換部２３は、受信パケットにかかる通信セションが既に不正侵入と認識されているので、その宛先アドレス「０２」を仮想おとりサーバ２２のＩＰアドレス「０４」に書き換えて転送する。

【００３１】仮想おとりサーバ２２は、当該パケットを受信して所定の処理を実行すると、発信元アドレスが自身のＩＰドレス「０４」、宛先アドレスが不正利用者端末３ｂのＩＰドレス「０５」であるパケットを返送する。経路切換部２３は、受信パケットの発信元アドレス「０５」を情報管理サーバ２のＩＰアドレス「０２」に書き換えて返送する。

【００３２】このように、本実施形態によれば、不正侵入と判定された通信セッションのパケットは、その宛先アドレスが仮想おとりサーバ２２のアドレスへ書き換えられるので、仮想正規サーバ２１への侵入を防止できる。

【００３３】また、不正侵入者は仮想おとりサーバ２２に侵入しているにもかかわらず、仮想正規サーバ２１への侵入に成功したものと勘違いし、比較的長時間にわたって接続を維持するので、その間を利用して行動ログや追跡データの収集が可能になる。

【００３４】さらに、仮想おとりサーバ２２は仮想正規サーバ２１のコピーにより構築することができるので、その構築が極めて容易になる。また、各サーバのディレクトリ構造を実質的に同一にできるので、不正侵入者のアクセスを仮想おとりサーバ２２へ誘導し、この仮想おとりサーバ２２から不正侵入者に対して応答を返信しても、この応答に含まれるアクセス先のディレクトリ情報に基づいて、仮想おとりサーバへの誘導すなわち不正侵入の失敗を悟られることがない。

【００３５】図６は、本発明が適用される不正侵入防止システムの第２実施形態の構成を示したブロック図であり、前記と同一の符号は同一または同等部分を表している。

【００３６】通信ネットワーク１には、正規サーバ６１およびおとりサーバ６２が、経路切換部６３を介して接続されている。不正侵入検知部６４は、不正侵入を前記と同様に検知して経路切換部６３へ通知する。経路切換部６３は、例えばルータであり、不正侵入検知部６４による不正侵入の検知結果に基づいて、各通信端末３からのアクセスを、正規サーバ６１およびおとりサーバ６２の双方、またはおとりサーバ６２のみへ選択的に誘導する。

【００３７】次いで、本実施形態の動作を、図７に示した通信シーケンスを参照して説明する。

【００３８】正規利用者の通信端末３ａから正規サーバ６１に宛てて送出されたパケット（コマンド）、あるいは不正侵入が検知されるまでに不正利用者の通信端末３ｂから正規サーバ６１に宛てて送出されたパケット［同図(a)］は、経路切換部６３において、正規サーバ６１およびおとりサーバ６２の双方［同図(b)、(c)］へ同時に誘導される。正規サーバ６１およびおとりサーバ６２は、受信パケットの内容に応答した処理を実行し、自身に固有のタイミングで経路切換部６３へ応答をそれぞれ返送する［同図(d)、(e)］。

【００３９】図７に示した例では、経路切換部６３は正規サーバ６１から先に応答を受信［同図(d)］するが、これを直ちには返送せず、おとりサーバ６２からの応答が受信されるまで待機する。おとりサーバ６２からの応答が受信［同図(e)］され、各サーバからの応答パケットが揃うと、正規サーバ６１から返送された応答を通信端末３に宛てて返送［同図(f)］する。

【００４０】以下同様に、経路切換部６３は通信端末３ａから正規サーバ６１に宛てて送出されたパケットを正規サーバ６１およびおとりサーバ６２の双方へ同時に転送する。そして、各サーバ６１，６２からの応答が揃うと、正規サーバ６１からの応答のみを通信端末３に宛てて返送する。

【００４１】その後、不正侵入検知部６４により不正侵入が検知されると、これが経路切換部６３へ通知［同図(g)］される。不正侵入検知部６４は、不正侵入が検知された以降は、通信端末３ａから正規サーバ６１に宛てて送出されたパケット［同図(h)］をおとりサーバ６２のみへ転送［同図(i)］し、おとりサーバ６２から返送された応答［同図(j)］を通信端末３に宛てて返送［同図(k)］する。

【００４２】本実施形態によれば、通信端末３から正規サーバ６１に宛てて送出されたパケットは、正規サーバ６１のみならずおとりサーバ６２へも転送されるので、各サーバ６１，６２の内容を整合させることができる。

【００４３】また、各サーバ６１，６２から返送される応答が揃った以降に、すなわち各サーバが受信パケットに対する処理を完了して両者の整合性が確保された以降に送信端末３へ応答が返信される。したがって、不正侵入者が先に、例えばｃｄコマンド（ディレクトリ切換）を実行し、その後、不正侵入の検知後に他のコマンドを更に実行したような場合、不正侵入者は、今回のコマンドに対しては前回のコマンドの内容が反映された応答を受信できる。したがって、不正侵入者はおとりサーバ６２に侵入しているにもかかわらず、正規サーバ６１への侵入に成功したものと勘違いし、比較的長時間にわたって接続を維持するので、その間を利用して行動ログや追跡データの収集が可能になる。さらに、不正侵入者には正規サーバ６１への侵入に失敗したことを悟られないので、この不正侵入者による再度の侵入行為や他の妨害行為、破壊行為、迷惑行為等を防止できる。

【００４４】図８は、本発明を適用した不正侵入防止システムの第３実施形態の構成を示したブロック図であり、前記と同一の符号は同一または同等部分を表している。

【００４５】情報管理サーバ８は、正規サーバとして機能する正規データ領域８１、およびおとりサーバとして機能するおとりデータ領域８２を含み、各データ領域８１、８２は、通信ネットワーク１を介して通信端末３と接続されている。

【００４６】図９は、前記情報管理サーバ８の構成を示したブロック図であり、前記と同一の符号は同一または同等部分を表している。

【００４７】インターフェース（Ｉ／Ｆ）８４は、当該情報管理サーバ８と通信ネットワーク１との物理的な接続、および当該情報管理サーバ８が実行する通信アプリケーションと通信端末３が実行する通信アプリケーションとの通信を制御する。不正侵入監視部８５は、当該情報管理サーバ８への不正侵入を検知し、その旨を通信アプリケーション部８３へ通知する。

【００４８】通信アプリケーション部８３は、アプリケーションレイヤにおいてアクセス要求を解釈し、宛先として指定されているデータ領域（正規データ領域８１またはおとりデータ領域８２）にアクセスし、さらに、その応答をインターフェース８４へ返す。

【００４９】次いで、本実施形態の動作を、図１０に示した通信シーケンスを参照して説明する。

【００５０】正規利用者の通信端末３ａから、あるいは不正侵入が検知されるまでに不正利用者の通信端末３ｂから、情報管理サーバ８に対して接続要求［同図(a)］が発せられると、情報管理サーバ８の通信アプリケーション部８３は、この接続要求に対して応答を返信［同図(b)］する。その後、所定の認証処理等が実行されて両者に間に通信セションが確立される。

【００５１】その後、通信端末３から正規データ領域８１に宛ててパケット（コマンド）が送信［同図(c)］されると、これが通信アプリケーション部８３を経由して正規データ領域８１へ転送［同図(d)］される。正規データ領域８１は、受信パケットで指示されたコマンドを実行し、その応答を返信［同図(e)］する。この応答は、通信アプリケーション部８３およびネットワークインターフェース８４を経由して通信端末３へ返送［同図(f)］される。

【００５２】その後、前記不正侵入検知部８５により不正侵入が検知され、これがインターフェース８４へ通知［同図(g)］されると、インターフェース８４は通信アプリケーション部８３に対して終了要求［同図(h)］を送信する。インターフェース８４は、前記終了要求に対

する応答を受信［同図(i)］すると、おとりデータ領域８２を指定してコマンド「chroot」をコールする。

【００５３】図１１は、前記情報管理サーバ８のディレクトリ構造の一例を示した図であり、本実施形態では、ルートディレクトリの下に「home」、「bin」、「dev」、「var」および「etc」の各ディレクトリが存在し、ディレクトリ「home」の下に、おとりデータ領域の最上位ディレクトリである「decoy」が確保されている。ディレクトリ「decoy」の下には、「home」、「bin」、「var」の各ディレクトリが存在する。したがって、おとりデータ領域８２のディレクトリ「wtmp」は、home／decoy／var／log／wtmpと定義できる。

【００５４】これに対して、正規データ領域８１は、ルートディレクトリの下のディレクトリ「var」の下に構築されているので、そのディレクトリ「wtmp」は、var／log／wtmpと定義できる。 すなわち、前記おとりデータ領域８２は、前記正規データ領域８１のルートディレクトリ以下のディレクトリ構造に対応あるいは実質的に同一のディレクトリ構造を、ディレクトリ「decoy」以下に有している。

【００５５】ここで、前記コマンド「chroot」がおとりデータ領域８２を指定してコールされると、おとりデータ領域８２の最上位ディレクトリ「decoy」がルートディレクトリとなり、その上位ディレクトリが全てマスクされる。したがって、おとりデータ領域８２の前記ディレクトリ「wtmp」は、前記コマンド「ｃｈｒｏｏｔ」がコールされると、正規データ領域８１の場合と同様に、var／log／wtmpと定義されることになる。

【００５６】図１０に戻り、前記コマンド「chroot」のコール後は、インターフェース８４が通信アプリケーション部８３に対して接続要求を送信［同図(j)］する。インターフェース８４は、この接続要求に対する応答を受信［同図(k)］すると、その後に当該不正侵入端末３から送信されるパケットを、全ておとりデータ領域８２へ誘導［同図(l)］する。

【００５７】おとりデータ領域８２は、受信コマンドを実行して応答を返送［同図(m)］するが、おとりデータ領域８２と正規データ領域８１とは、不正侵入者から見たディレクトリ構造が実質的に同一なので、その応答に含まれるディレクトリ情報も、正規データ領域８１からの応答に含まれるであろうディレクトリ情報と何ら変わりない。したがって、応答をそのまま通信端末へ返信しても、これがおとりデータ領域８２からの応答であることを不正侵入者に見破られることがない。

【００５８】このように、本実施形態によれば、正規データ領域８１およびデータ領域８２のディレクトリ構造が、不正侵入者等の外部からのアクセス者に対しては同一となるので、不正侵入者のアクセスをおとりデータ領域８２へ誘導し、当該おとりデータ領域８２から不正侵入者に対して応答しても、この応答に含まれるアクセス先（おとりデータ領域８２）のディレクトリ情報に基づいて、不正侵入の失敗を悟られることがない。

【００５９】

【発明の効果】本発明によれば、以下のような効果が達成される。

【００６０】(1)一つのハードウエア上に、エミュレータを用いて仮想正規サーバと仮想おとりサーバとを設け、各サーバのディレクトリ構造を同一としたので、不正侵入者のアクセスを仮想おとりサーバへ誘導し、当該仮想おとりサーバから不正侵入者に対して応答を返信しても、この応答に含まれるアクセス先のディレクトリ情報に基づいて、仮想おとりサーバへの誘導すなわち不正侵入の失敗を悟られることがない。また、仮想おとりサーバは、仮想正規サーバの内容をコピーするだけで簡単に構築することができる。

【００６１】(2)正規サーバへのアクセスを、不正侵入が検知されるまでは正規サーバのみならずおとりサーバへも転送すると共に、正規サーバからアクセス元への応答は、正規サーバおよびおとりサーバからの応答が揃ってから返送するようにしたので、次にアクセスされるタイミングでは、正規サーバとおとりサーバとの整合性を保つことができる。したがって、不正侵入が検知された以降のアクセスをおとりサーバのみへ誘導し、このおとりサーバからアクセス元へ応答するようにしても、おとりサーバへの誘導すなわち不正侵入の失敗を、各サーバの内容が不整合であることに基づいて悟られることがない。

【００６２】(3)不正侵入が検知されると、おとりデータ領域を指定してchrootをコールすることにより、正規データ領域とおとりデータ領域とのディレクトリ構造が、外部からのアクセス者に対しては同一となるので、不正侵入者のアクセスをおとりデータ領域へ誘導し、当該おとりデータ領域から不正侵入者に対して応答しても、この応答に含まれるアクセス先のディレクトリ情報に基づいて、不正侵入の失敗を悟られることがない。

【図面の簡単な説明】

【図１】 本発明を適用した不正侵入防止システムの第１実施形態のブロック図である。

【図２】 図１の情報管理サーバの構造を模式的に示したブロック図である。

【図３】 仮想正規サーバおよび仮想おとりサーバのディレクトリ構造を示した図である。

【図４】 第１実施形態の正規利用者によるアクセス時の通信シーケンスを示した図である。

【図５】 第１実施形態の不正利用者によるアクセス時の通信シーケンスを示した図である。

【図６】 本発明を適用した不正侵入防止システムの第２実施形態のブロック図である。

【図７】 第２実施形態の通信シーケンスを示した図である。

11

【図８】　本発明を適用した不正侵入防止システムの第３実施形態のブロック図である。

【図９】　第３実施形態の通信シーケンスを示した図である。

【図１０】　図９の情報管理サーバの構造を模式的に示したブロック図である。

【図１１】　第３実施形態における正規データ領域およびおとりデータ領域のディレクトリ構造を示した図である。

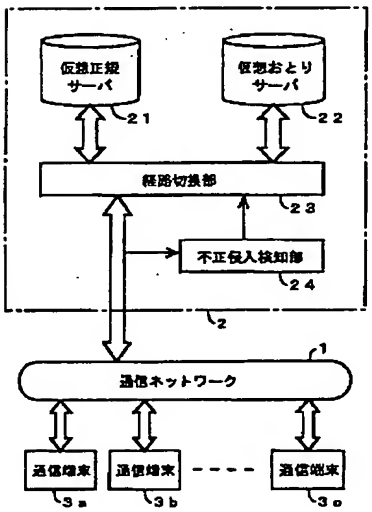
【符号の説明】

12

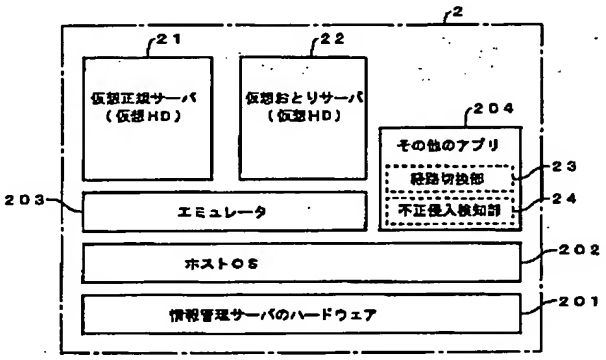
＊１…通信ネットワーク、２、８…情報管理サーバ、３…通信端末、２１…仮想正規サーバ、２２…仮想おとりサーバ、２３、６３…経路切換部、２４，６４，８５…不正侵入検知部、６１…正規サーバ、６２…おとりサーバ、８１…正規データ領域、８２…おとりデータ領域、８３…通信アプリケーション部、８４…インターフェース（Ｉ／Ｆ）、２０１…情報管理サーバのハードウエア、２０２…情報管理サーバのホストＯＳ、２０３…エミュレータ、２０４…アプリケーション

＊10

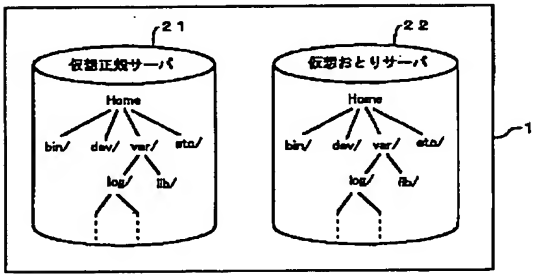
【図１】



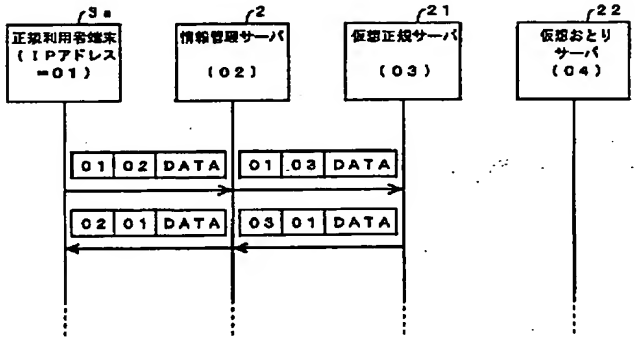
【図２】



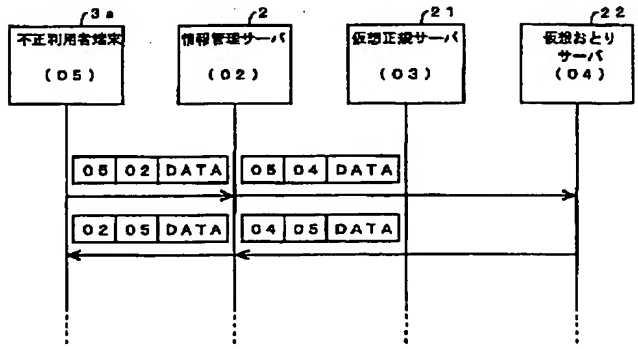
【図３】



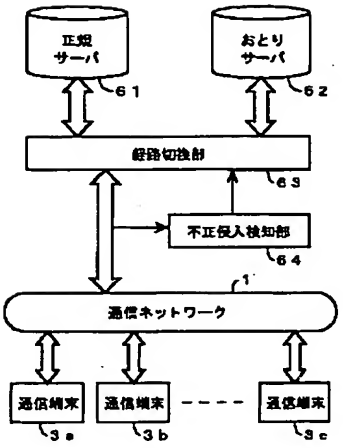
【図４】



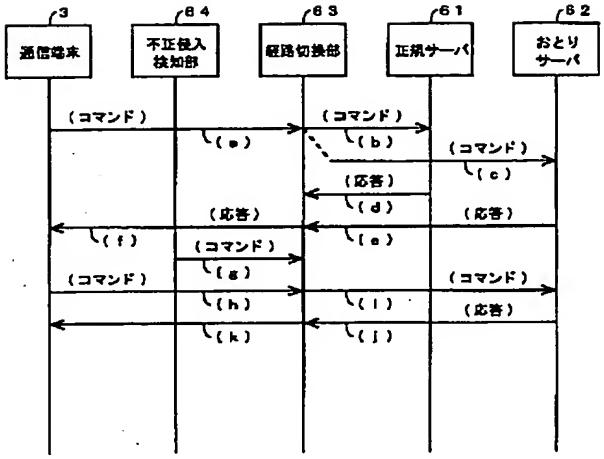
【図５】



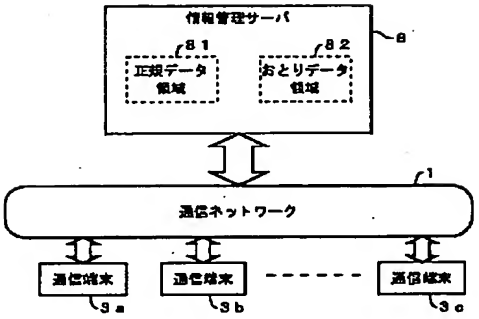
【図６】



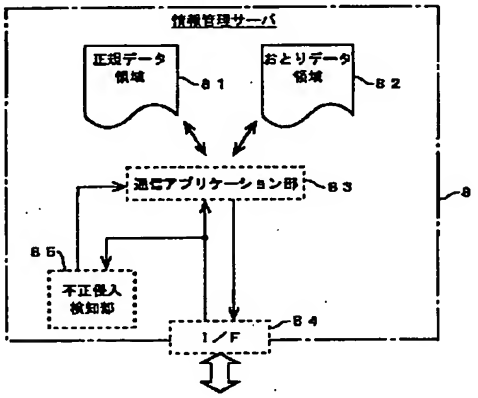
【図７】



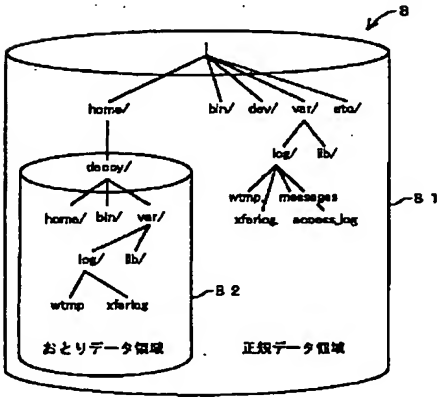
【図８】



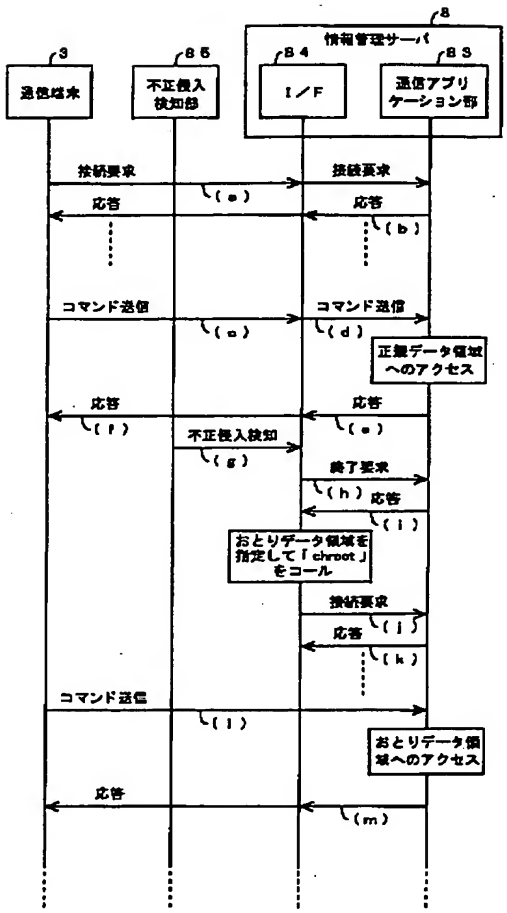
【図９】



【図１１】



【図１０】



フロントページの続き

(72)発明者　清本　晋作
埼玉県上福岡市大原二丁目１番15号　株式会社ケイディーディーアイ研究所内

(72)発明者　中尾　康二
埼玉県上福岡市大原二丁目１番15号　株式会社ケイディーディーアイ研究所内

Ｆターム(参考)　5B085 AE00
5K030 GA15 HC01 HC13 HD03 HD06
LB08 LD11